

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-236147

(43)Date of publication of application : 23.08.1994

(51)Int.Cl.

G09C 1/00
G06K 17/00

(21)Application number : 05-044432

(71)Applicant : PANPUKIN HOUSE:KK

(22)Date of filing : 10.02.1993

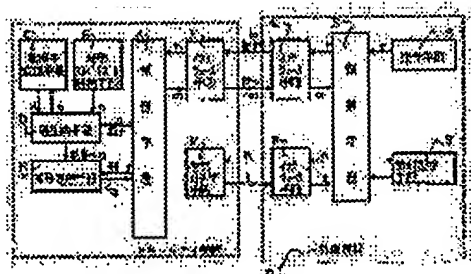
(72)Inventor : IMAI HIDEKI

(54) SECURITY DEVICE

(57)Abstract:

PURPOSE: To prevent to write in and read out illegally information of magnetic stripes, while cryptographic processing is enabled without a previous arrangement and delivery of a cryptographic key by inputting an identifier of a specific entity and generating the cryptographic key by a key generating means.

CONSTITUTION: A control means A of this device takes out an identifier (a) of a partner entity out of indication information (b) inputted from an interface means N and sends it to a key generation means D. And a peculiar cryptographic key (e) being common with the partner entity is generated by operating an identifier (d) to which the identifier (a) is converted by an identifier exchanging means C and a secret algorithm (c) stored in a secret algorithm storing means B, and sent to a cryptographic processing means E. Also, information written in a magnetic stripe means M of this device is sent to the cryptographic processing means E of this device from an external device O, ciphered by using the cryptographic key (e), made ciphered information (q), and returned to the external device O from the interface means N as a response (m).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-236147

(43)公開日 平成6年(1994)8月23日

(51)Int.Cl.⁵

G 0 9 C 1/00

G 0 6 K 17/00

識別記号

庁内整理番号

8837-5L

T 7459-5L

F I

技術表示箇所

審査請求 未請求 請求項の数 3 F D (全 6 頁)

(21)出願番号 特願平5-44432

(22)出願日 平成5年(1993)2月10日

(71)出願人 393009356

株式会社バンブキンハウス

神奈川県厚木市飯山1620番地の1 アメニ

ティヒル本厚木717

(72)発明者 今井 秀樹

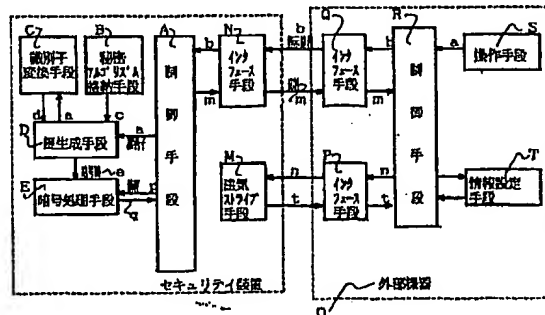
神奈川県横浜市区六ツ川3-76-3-J
902

(54)【発明の名称】 セキュリティ装置

(57)【要約】 (修正有)

【目的】 本発明は、任意に定めることのできる公開された相手エンティティの識別子を自分の秘密アルゴリズムに入力するだけで相手エンティティと自分に固有の暗号鍵を生成する鍵共有方式暗号システム(KPS)による鍵生成手段を用いて暗号鍵を生成させ、この鍵を用いて磁気ストライプ上の情報を暗号化して記録及び/または読みだして復号することにより磁気ストライプ上のセキュリティを確保するセキュリティ装置を実現する。

【構成】 秘密アルゴリズムを格納する秘密アルゴリズム格納手段と、エンティティの識別子を変換する識別子変換手段と、識別子変換手段の出力と秘密アルゴリズム格納手段から暗号鍵を生成する鍵生成手段と、鍵生成手段で生成した暗号鍵を用いる暗号処理手段と磁気ストライプ手段で構成する。



【特許請求の範囲】

【請求項1】 各エンティティ（人、装置など）が公開の識別子を有し、センタ（管理者）が、センタだけが持つ特別なアルゴリズム（情報）とエンティティの識別子に一方方向性でランダムな単射を行う識別子変換を施したものとを演算させてエンティティに固有な秘密アルゴリズム（情報）を生成し、これを格納する秘密アルゴリズム格納手段と、前記識別子変換手段と、任意のエンティティの識別子を前記識別子変換手段で変換したものと前記秘密アルゴリズムを演算させて自分と任意のエンティティに固有の暗号鍵（鍵）を生成させる鍵生成手段と、暗号処理手段と、磁気ストライプ手段を具備して、前記磁気ストライプ手段に記録される及び／または記録された情報を、前記鍵生成手段で生成した暗号鍵を用いて前記暗号処理手段で暗号化及び／または復号することの特徴とするセキュリティ装置。

【請求項2】 複数の前記秘密アルゴリズム格納手段を有し、それらから任意の秘密アルゴリズムを用いて暗号鍵の生成を行うことを特徴とする請求項1のセキュリティ装置。

【請求項3】 記憶手段をさらに具備したことを特徴とする請求項1及び請求項2のセキュリティ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、セキュリティ装置に関する。

【0002】

【従来技術】 情報の暗号化／復号を行う暗号装置がある。また、磁気ストライプを有するカードが普及している。

【0003】

【発明が解決しようとする問題点】 キャッシュカード、クレジットカード、プリペイドカードなどが、磁気ストライプを有するカード（磁気ストライプカード）として普及しているが、磁気ストライプ上の情報は不正にコピーすることができ、情報保全上に問題がある。また、種々の情報を記録するICカードなどがあるが、これには情報の漏洩などの問題がある。さらに、情報保全のため、暗号機能を内蔵させて情報の暗号化と復号を行う暗号装置が実現されているが、これには通信を行う当事者間で暗号鍵の打合わせが必要であり、さらにその鍵を安全に保管する為の管理が必要となる。

【0004】

【課題を解決する為の手段】 本発明は、各エンティティ（人、装置など）が公開の識別子を有し、センタ（管理者）が、センタだけが持つ特別なアルゴリズム（情報）とエンティティの識別子に一方方向性でランダムな単射を行う識別子変換を施したものとを演算させてエンティティに固有な秘密アルゴリズム（情報）を生成し、これを格納する秘密アルゴリズム格納手段と、前記識別子変換

手段と、任意のエンティティの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム（以下、KPSという）の理論を用いた鍵生成手段と、暗号処理手段と、磁気ストライプ手段を具備し、特定のエンティティの識別子を入力して前記識別子変換手段を施したものと前記秘密アルゴリズムとを演算させて暗号鍵（鍵）を生成させ、この鍵を用いて前記磁気ストライプの情報を前記暗号処理手段で暗号化して記録及び／または読み出して復号することにより、前記磁気ストライプの情報を不正に書込むことや読み出すことを防ぐセキュリティ装置を実現する。

【0005】 さらに、記憶手段を具備することにより格納する及び／または格納された情報を、前記鍵生成手段で生成した暗号鍵と前記暗号処理手段で暗号化及び／または復号してこれらの情報に対する不正な書込みや読み出しを防止することを可能としている。また、複数の秘密アルゴリズム格納手段を具備し、秘密アルゴリズムを複数内蔵してそれらから任意の1つを用いて暗号鍵生成を行うことにより、本発明によるセキュリティ装置を複数のエンティティで共用することや、一人のエンティティが複数の識別子を持ちそれぞれの識別子に対応する秘密アルゴリズムを有することや、異なる複数のセンタのアルゴリズムで生成された複数の秘密アルゴリズムを持つことが可能なセキュリティ装置を実現した。

【0006】

【実施例】 図1は、本発明請求項1のセキュリティ装置（以下、本装置という）の一実施例で、本装置とそれを用いる外部機器Oの構成例及びその動作を説明する図である。本装置は、制御手段A、秘密アルゴリズム格納手段B、識別子変換手段C、秘密アルゴリズムと識別子変換手段Cの出力から暗号鍵を生成する鍵生成手段D、鍵生成手段Dで生成した暗号鍵を用いて情報の暗号化／復号を行う暗号処理手段E、磁気ストライプ手段M及び外部機器Gと情報の送受信を行うインタフェース手段Nで構成される。外部機器Oは、制御手段R、本装置のインタフェース手段Nを接続するインタフェース手段Q、本装置の磁気ストライプ手段Mの情報を書込む又は読み出すためのインタフェース手段P、各種操作や情報入力を行う操作手段S、操作手段Sやインタフェース手段Pから入力された情報を設定する情報設定手段Tで構成される。ここで、制御手段A、並びにR、暗号処理手段E、識別子変換手段C、鍵生成手段DはCPU、メモリ及びプログラム、秘密アルゴリズム格納手段Bはメモリで構成することができる。

【0007】 本装置と外部機器Oを用いて、磁気ストライプの情報を暗号化して書込み、又は読み出して復号することにより不正な書込みや読み出しを防止する処理について図1により説明する。外部機器Oの操作手段Sから入力された相手エンティティ（人、装置）の識別子aは、制御手段Rにより指示情報bとしてインタフェース

手段Qを経て本装置のインタフェース手段Nに送られる。本装置の制御手段Aは、インタフェース手段Nから入力された前記指示情報bより前記識別子aを取り出して鍵生成手段Dに送り、これを識別子変換手段Cで変換したdと秘密アルゴリズム格納手段Bに格納された秘密アルゴリズムoとを演算させて相手エンティティとの固有な暗号鍵eを生成させ、暗号処理手段Eに送る。また、本装置の磁気ストライプ手段Mに書込む情報は、外部機器Oから本装置の暗号処理手段Eに送られ前記暗号鍵eを用いて暗号化されて暗号化情報qとなり、インタフェース手段Nより応答mとして外部機器Oへ返される。外部機器Oの制御手段Rは、インタフェース手段Qで受信した前記応答mから暗号化情報qを取り出して本装置の磁気ストライプ手段Mへの書込みを行う。また、前記磁気ストライプ手段Mに書込まれた暗号化情報tは、インタフェース手段Pで読み出されて本装置の暗号処理手段Eに送られ前記暗号鍵eを用いて復号されて復号情報qとなり、インタフェース手段Nより応答mとして制御手段Rへ返される。

【0008】ここで、本発明が使用している打合せや第三者による暗号鍵(鍵)の配送を必要とせずに、自分と任意のエンティティに固有の鍵を生成するKPSについて説明する。エンティティiが、半固定的に用いるもので任意に定められる公開の識別子を有し、これを識別子 Y_i とし、これに一方方向性でランダムな単射を行う識別子変換Fを施したものを Z_i (数式1)とする。センタだけが持つ特別なアルゴリズム(情報)Gと、前記 Z_i とを演算させて、エンティティiに固有な秘密アルゴリズム(情報) X_i (数式2)を生成する。

【数1】

【数2】エンティティiは、自分の秘密アルゴリズム X_i にエンティティjの識別子 Y_j を識別子変換したものの Z_j を入力し、演算させて(数式3)、エンティティjとの共通な暗号鍵 k_{ij} を生成させることができる。またエンティティjの秘密アルゴリズム X_j に、エンティティiの識別子 Y_i を識別子変換した Z_i を入力して演算し(数式4)、鍵 k_{ji} を生成させることができ、これが前記 k_{ij} に等しい(数式5)ので、エンティティiが暗号鍵 k_{ij} で暗号化した内容は、エンティティjに復号させることができる。

【数3】

【数4】

【数5】KPSの理論的な詳細については、文献1から文献5等に記述されている。

【0009】図2は、本発明請求項2の一実施例とその動作を示す図である。図中A及びCからT、aからqは図1と同じである。本発明請求項2のセキュリティ装置は、複数の秘密アルゴリズム格納手段を示す秘密アルゴリズム格納手段A(B1)、秘密アルゴリズム格納手段イ(B2)と、選択手段Uとをさらに具備している。暗

号鍵生成時に制御手段Aからの制御情報rにより、選択手段Uは複数の秘密アルゴリズム格納手段から一つを選択して鍵生成手段Dに転送する。

【0010】図3は、本発明請求項3の一実施例とその動作を示す図である。図中AからT、aからqは図1と同じであり、さらに記憶手段Vを具備する。記憶手段Vの情報を、鍵生成手段Dで生成した暗号鍵eと暗号処理手段Eで暗号化して外部装置Oに送り、これを外部装置Oが磁気ストライプ手段Mに書込むことにより記憶手段Vの情報を不正な書込みや読み出しの困難な暗号情報として磁気ストライプ手段に記録すると共に、これを外部装置Oが読みだして本装置に送って復号させ、予め記憶手段Vに記憶した情報と照合させることなどができる。

【0011】

【発明の効果】本発明によるセキュリティ装置は、任意のエンティティの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム(以下、KPSという)の理論を用いた鍵生成手段と、識別子変換手段と、秘密アルゴリズム格納手段を、暗号処理手段と磁気ストライプ手段を持った装置に内蔵させ、特定のエンティティの識別子を入力して前記鍵生成手段で暗号鍵(鍵)を生成させ、この鍵を用いて磁気ストライプの情報を前記暗号処理手段で暗号化して書込み、または読み出して復号することにより、磁気ストライプの情報を不正に書込むことや読み出すことを防ぐと共に暗号鍵の打合せや配送を不要として暗号処理を行うことを可能とした。

【0012】また、複数の秘密アルゴリズム格納手段をさらに具備し、秘密アルゴリズムを複数内蔵してそれから任意の1つを選択することにより、複数のエンティティで共用するセキュリティ装置や、一人のエンティティが複数の識別子を持ちそれぞれの識別子に対応する秘密アルゴリズムを有したセキュリティ装置や、異なる複数のセンタのアルゴリズムで生成された複数の秘密アルゴリズムを内蔵してセンタのアルゴリズムの更新に対応することや、異なるセンタ間での共有鍵の生成が可能なセキュリティ装置を実現する。さらに、記憶手段を具備してこれに格納する、または格納された情報を、前記暗号鍵生成手段で生成した暗号鍵と前記暗号処理手段により暗号化または復号することによりこれらの情報を不正に書込むことや読み出すことを防ぐと共に、これを磁気ストライプ手段に記録することにより、磁気ストライプ上の情報を不正にコピーして悪用することを防ぐことが可能となる。

【0013】クレジットカード、キャッシュカード、プリペイドカード等従来磁気ストライプカードで実現しているこれらの機能は、本装置をカードで実現してその一端に磁気ストライプ手段Mを設定することにより、従来の磁気ストライプ用機器で本装置を利用することができる。

【図面の簡単な説明】

【図1】本発明請求項1の一実施例とその動作を説明する図である。

【図2】本発明請求項2の一実施例とその動作を説明する図である。

【図3】本発明請求項3の一実施例とその動作を説明する図である。

【符号の説明】

- A 制御手段
- B 秘密アルゴリズム格納手段
- B1 秘密アルゴリズム格納手段ア
- B2 秘密アルゴリズム格納手段イ
- C 識別子変換手段
- D 鍵生成手段
- E 暗号処理手段
- M 磁気ストライプ手段
- N インタフェース手段
- O 外部機器
- P インタフェース手段
- Q インタフェース手段
- R 制御手段
- S 操作手段
- T 情報設定手段
- U 選択手段
- V 記憶手段
- a 識別子
- b 指示情報
- c 秘密アルゴリズム情報
- d 識別子変換された情報
- e 暗号鍵
- m 応答
- n 書込み情報
- t 読みだし情報
- p 平文/暗号文情報
- q 暗号化/復号情報
- r 制御手段と選択手段間の制御情報

【数1】 $Z_i = F(Y_i)$

【数2】 $X_i = G(Z_i)$

【数3】 $k_{ij} = X_i(Z_j)$

【数4】 $k_{ji} = X_j(Z_i)$

【数5】 $k_{ij} = k_{ji} = k$

【文献1】松本勉、今井秀樹、"第3の鍵共有方式"、1986年暗号と情報セキュリティワークショップ講演論文集、1986年8月。

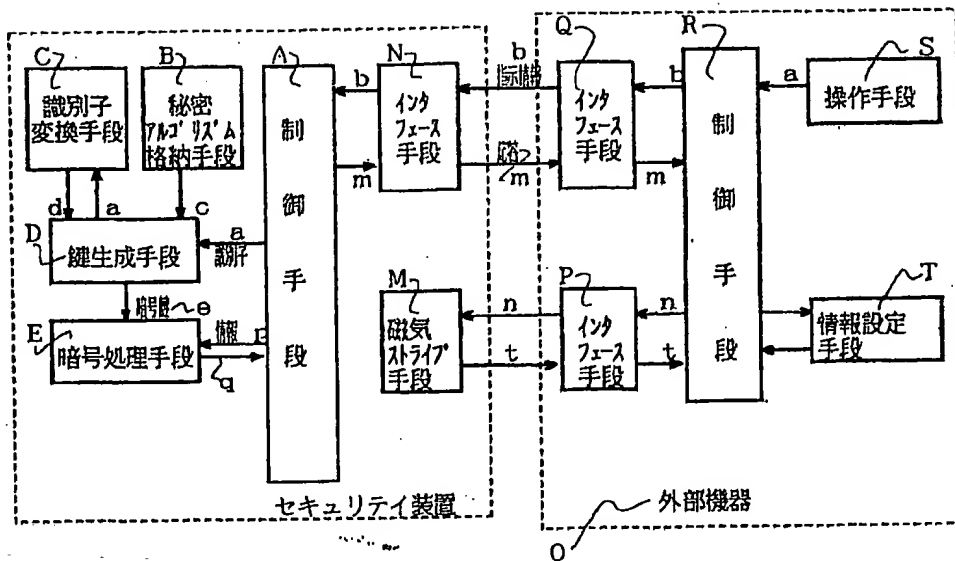
【文献2】松本勉、今井秀樹、"簡便な暗号鍵共有方式"、電気通信学会誌IT86-54、P-29~34、1986年9月。

10 【文献3】松本勉、今井秀樹、"キー プレディストリビューション システムの一方式" ("KEY PRE DISTRIBUTION SYSTEM BASED ON LINEAR ALGEBRA")、第9回情報理論とその応用シンポジウム、SITA' 86、1986年10月。

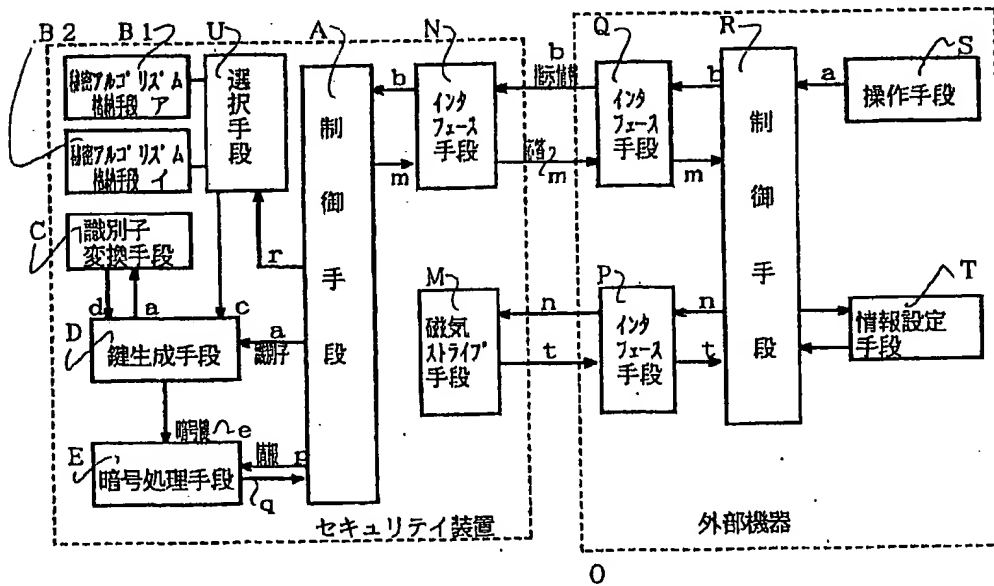
20 【文献4】松本勉、今井秀樹、"アプライング ザ キー プレディストリビューション システム トウ エレクトロニク メール アンド シグネチャ"、情報理論とその応用シンポジウム、SITA' 87、1987年11月。(Tsutomu MATSUMOTO and, Hideki IMAI, "Applying the Predistribution System to Electronic Mails and Signatures", SITA' 87, NO V., 1987.)

30 【文献5】松本勉、今井秀樹、"パフォーマンス オブ リニア スキーム フォア ザ キー プレディストリビューション システム"、IEICE情報セキュリティ技術報告、5月20日号、1989年。(Tsutomu MATSUMOTO and, Hideki IMAI, "Performance of linear schemes for the Key Predistribution System", IEICE Technical report on Information Security, May 20, 1988.)

【図1】



【図2】



【図3】

